



TURMOIL VPN PROCESSING

27 October 2009



The overall classification for this brief is:
[TOP SECRET//COMINT//REL TO USA, FVEY]



Agenda

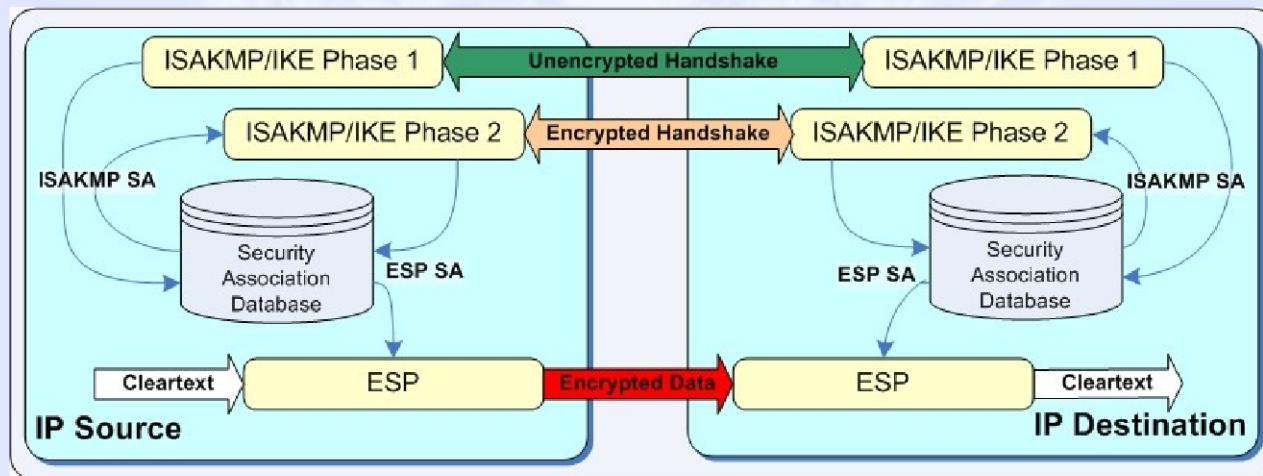
- VPN Technology Overview
- Dataflows and Interfaces
- LPT Implementation
- Metrics



Overview – VPN Mission Opportunity

(S//SI//REL) Exploit Virtual Private Network (**VPN**) communications that use IP Security (**IPsec**) algorithms and protocols:

- (U) **ISAKMP** – Internet Security Association and Key Management Protocol (RFC2407, RFC2408) provides an authentication and key exchange framework.
- (U) **IKE** – Internet Key Exchange (RFC2409) provides authentication and key exchange mechanisms.
- (U) **ESP** - Encapsulating Security Payload (RFC2406) provides traffic confidentiality (encryption) and optional integrity protection.
- (U) **AH** – Authentication Header (RFC2402) provides integrity protection that includes IP Header. Sometimes AH is used to wrap ESP for additional integrity.



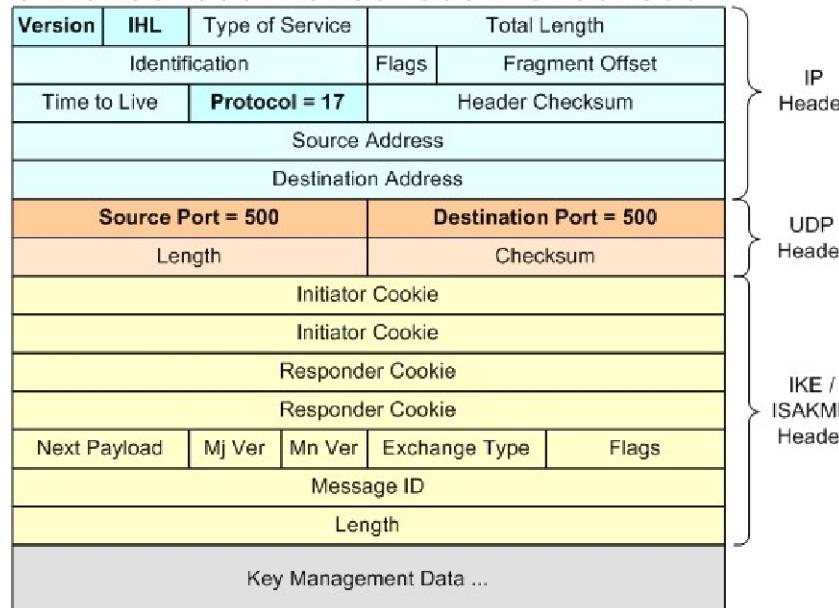


IKE-ISAKMP Protocol

UNCLASSIFIED

Internet Key Exchange (IKE – RFC 2409)
Internet Security Association and Key Management
Protocol (ISAKMP – RFC 2408)

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0	0 1 2 3 4 5 6 7 8 9 0	0 1 2 3 4 5 6 7 8 9 0	1



UNCLASSIFIED

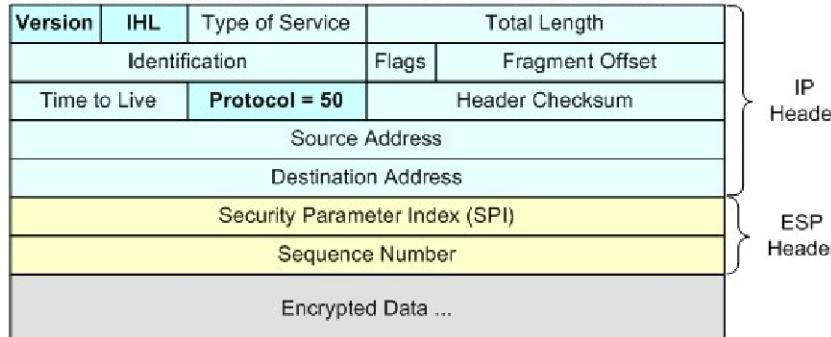


ESP Protocol

UNCLASSIFIED

Encapsulating Security Payload (ESP - RFC 2406)

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1



UNCLASSIFIED

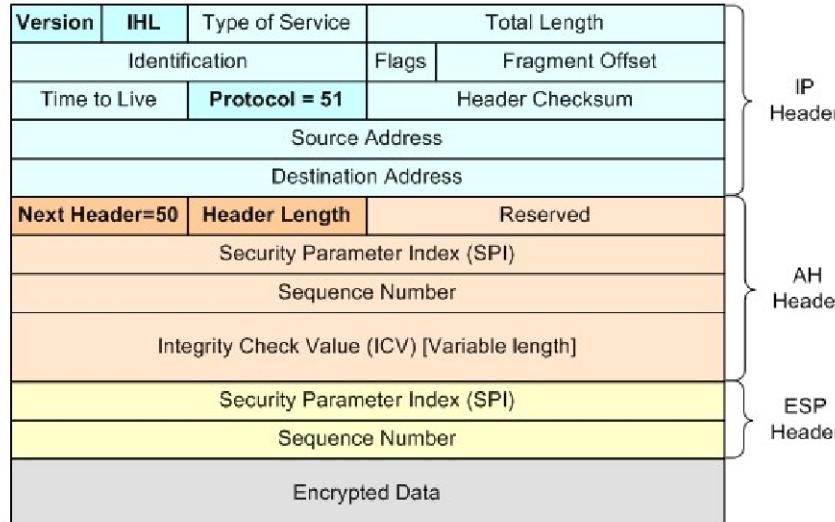


AH-ESP Protocol

UNCLASSIFIED

Authentication Header (AH – RFC 2402)
Encapsulating Security Payload (ESP - RFC 2406)

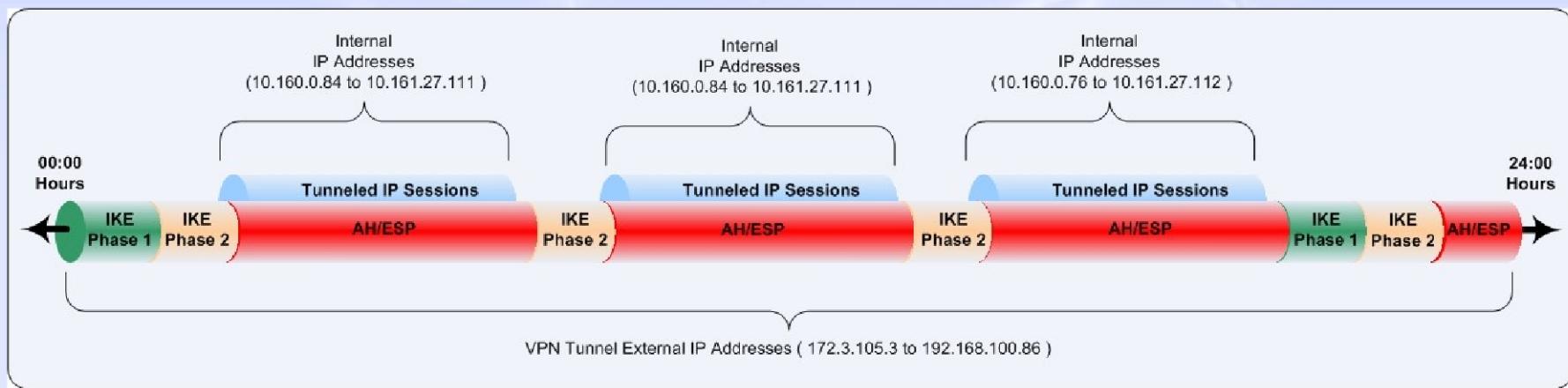
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1



UNCLASSIFIED



Overview – VPN IPsec Collection

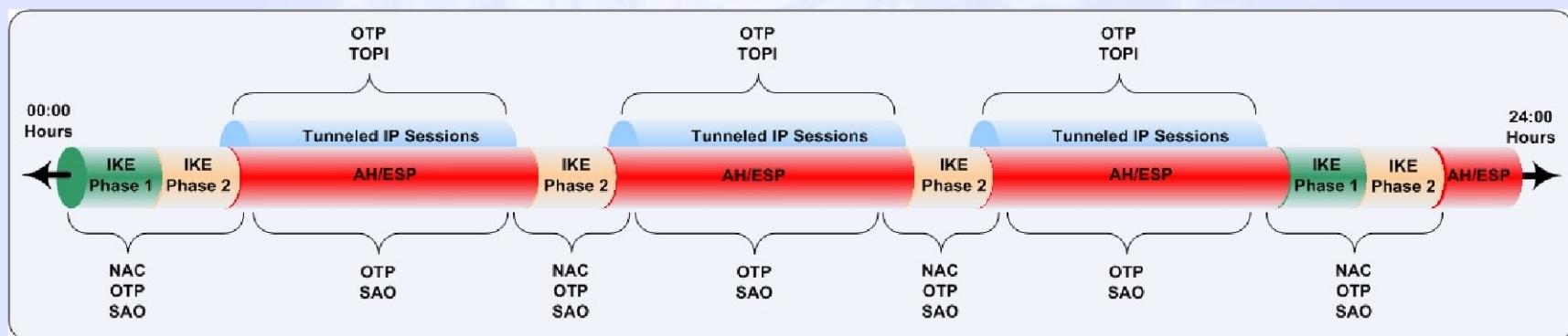


- (TS//SI//REL) Collection requires ***dwell time*** to capture IKE associated with ESP
- (TS//SI//REL) Collection requires ***link diversity*** to capture IKE associated with ESP
 - (S//SI//REL) There is no guarantee that IKE and ESP will use the same link.
- (S//SI//REL) Collection requires ***multiple selectors*** to target external and tunneled sessions
 - (S//SI//REL) VPN Tunnel External IP Addresses – To Target Decryption
 - (S//SI//REL) Strong Selectors on Internal IP Links – To Target VPN Content



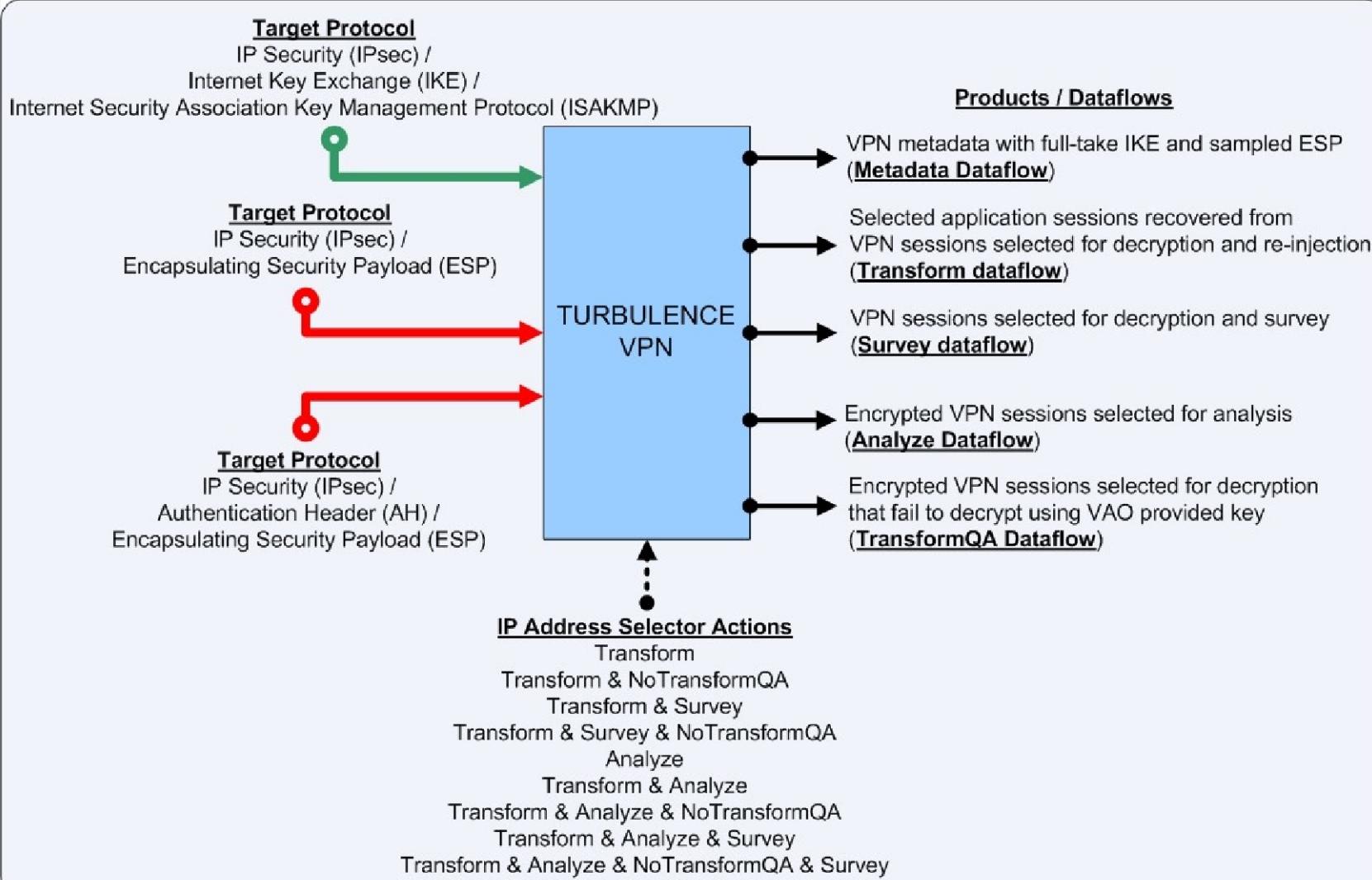
Overview – Customer Needs

Customer	Functions	Needs
SIGINT Analyst (TOPI)	<ul style="list-style-type: none"> •Target and Analyze Traffic •Report SIGINT 	<ul style="list-style-type: none"> •Target IDs, Target Links, Target Value •Unencrypted Targeted Traffic
Network Analysis Center (NAC)	<ul style="list-style-type: none"> •Identify target VPN's •Report VPN Target IDs and Links 	<ul style="list-style-type: none"> •VPN IKE and ESP Metadata
Office of Target Pursuit (OTP)	<ul style="list-style-type: none"> •Search and survey for VPN's of interest •Report VPN Traffic Intelligence Value 	<ul style="list-style-type: none"> •VPN IKE and ESP Metadata •VPN Encrypted Surveys •VPN Unencrypted Surveys
Systems Analysis Office (SAO)	<ul style="list-style-type: none"> •Identify VPN Technologies •Identify VPN Vulnerabilities •Support VPN Exploitation 	<ul style="list-style-type: none"> •VPN IKE and ESP Metadata •VPN Encrypted Surveys •VPN Decryption Quality





Overview – VPN Products





Overview – Needs and Products

Customer	Needs	Products
SIGINT Analyst (TOPI)	<ul style="list-style-type: none"> • Target IDs, Target Links, Target Value • Unencrypted Targeted Traffic 	<ul style="list-style-type: none"> • Transform Dataflow
Network Analysis Center (NAC)	<ul style="list-style-type: none"> • VPN IKE and ESP Metadata 	<ul style="list-style-type: none"> • Metadata Dataflow – IKE Fulltake • Metadata Dataflow – ESP Samples
Office of Target Pursuit (OTP)	<ul style="list-style-type: none"> • VPN IKE and ESP Metadata 	<ul style="list-style-type: none"> • Metadata Dataflow – IKE Fulltake • Metadata Dataflow – ESP Samples
	<ul style="list-style-type: none"> • VPN Encrypted Surveys • VPN Unencrypted Surveys 	<ul style="list-style-type: none"> • Analysis Dataflow • Survey Dataflow
Systems Analysis Office (SAO)	<ul style="list-style-type: none"> • VPN IKE and ESP Metadata 	<ul style="list-style-type: none"> • Metadata Dataflow – IKE Fulltake • Metadata Dataflow – ESP Samples
	<ul style="list-style-type: none"> • VPN Encrypted Surveys • VPN Decryption Quality 	<ul style="list-style-type: none"> • Analysis Dataflow • TransformQA Dataflow

The diagram illustrates the data flow and analysis process across three phases of a TUNNELLED IP SESSION. The timeline shows 00:00 Hours on the left and 24:00 Hours on the right.

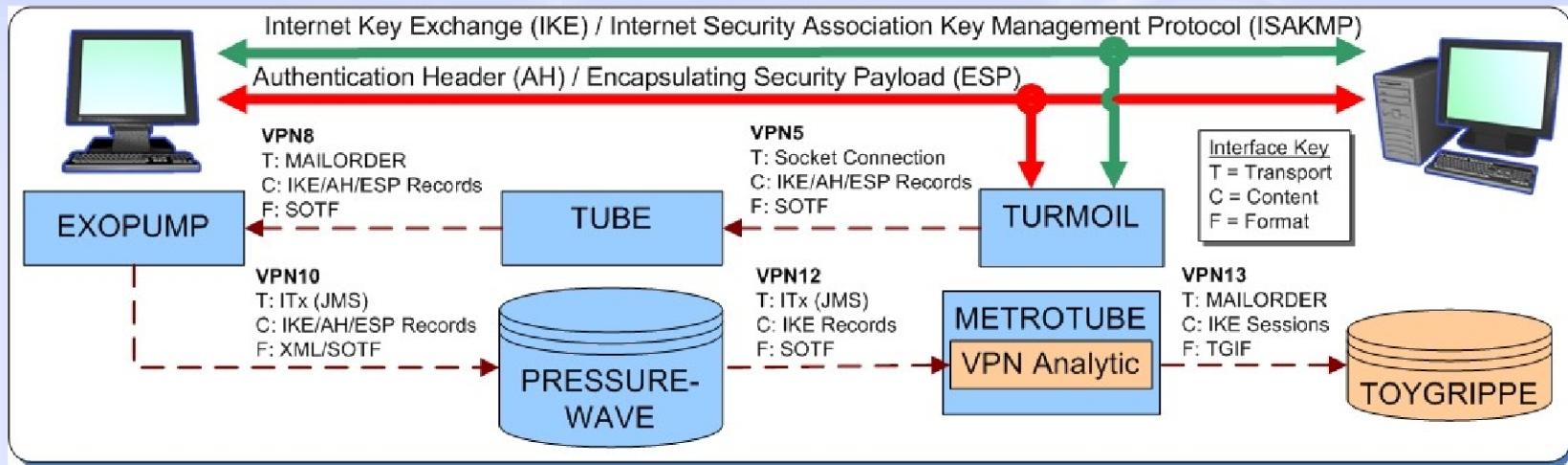
- Phase 1:** IKE Phase 1 (green) and AH/ESP (red).
- Phase 2:** IKE Phase 2 (red) and AH/ESP (red).
- Phase 3:** IKE Phase 1 (green) and AH/ESP (red).

Data flows from NAC, OTP, and SAO to various analysis and transform products:

- Transform Dataflow:** NAC, OTP, SAO (Phase 1), NAC, OTP, SAO (Phase 2), NAC, OTP, SAO (Phase 3).
- Survey Dataflow:** NAC, OTP, SAO (Phase 2).
- Analysis Dataflow:** NAC, OTP, SAO (Phase 1), NAC, OTP, SAO (Phase 2), NAC, OTP, SAO (Phase 3).
- TransformQA Dataflow:** NAC, OTP, SAO (Phase 3).



Dataflows and Interfaces - Metadata (Classic)



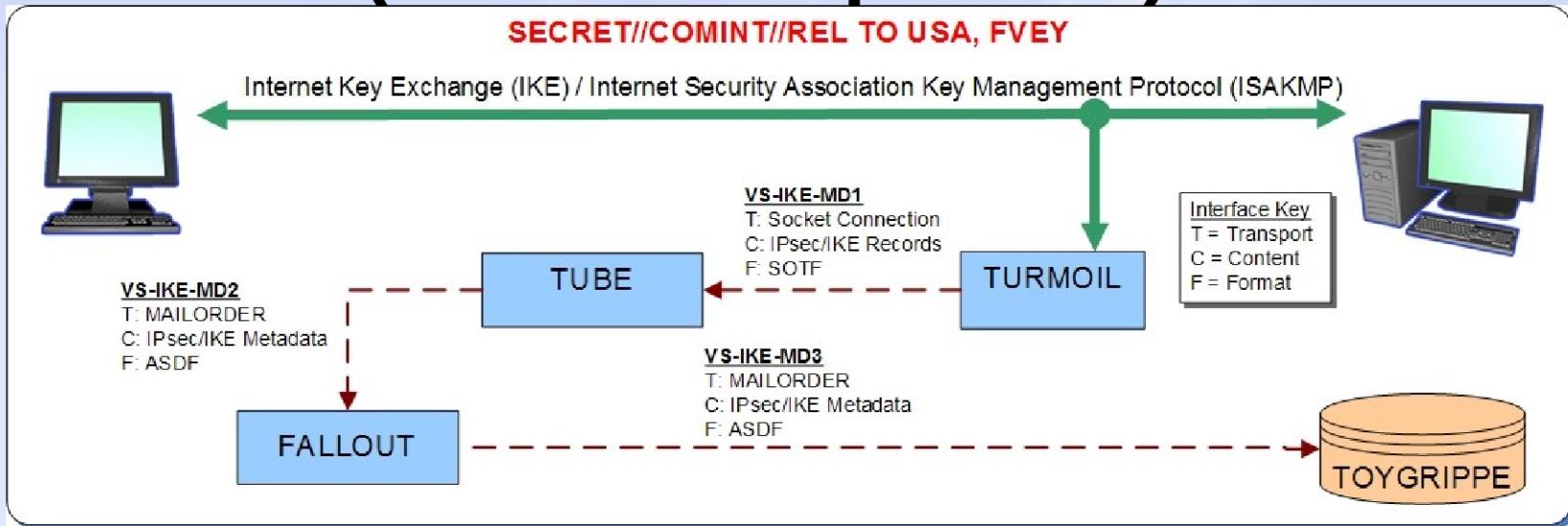
- (S//SI//REL) VPN IKE/ISAKMP Metadata in TOYGRIPPE is **full-take**
- (S//SI//REL) VPN ESP Metadata Sessions in PRESSUREWAVE is **sampled** (1/16th)
- (S//SI//REL) VPN AH/ESP Metadata Sessions in PRESSUREWAVE is **sampled** (1/16th)



Dataflows and Interfaces – IKE Metadata

(New and Improved!)

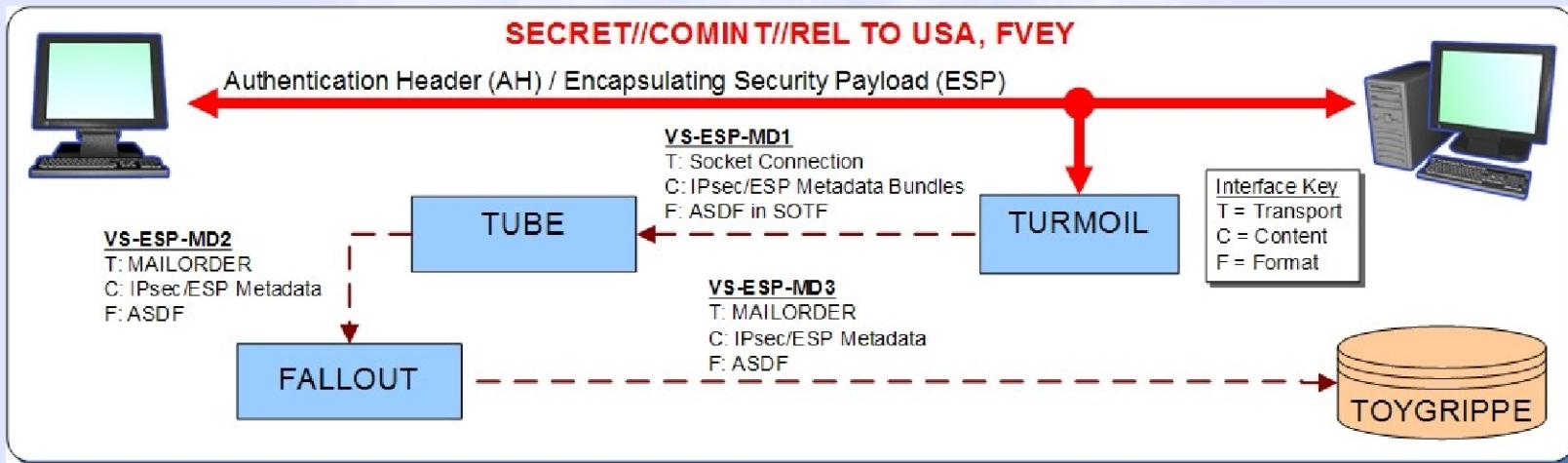
SECRET//COMINT//REL TO USA, FVEY



- (S//SI//REL) VPN IKE/ISAKMP Metadata in **TOYGRIPPE** is **full-take**
- (S//SI//REL) VPN ESP Metadata Sessions in **PRESSUREWAVE** is **sampled** (1/16th)
- (S//SI//REL) VPN AH/ESP Metadata Sessions in **PRESSUREWAVE** is **sampled** (1/16th)

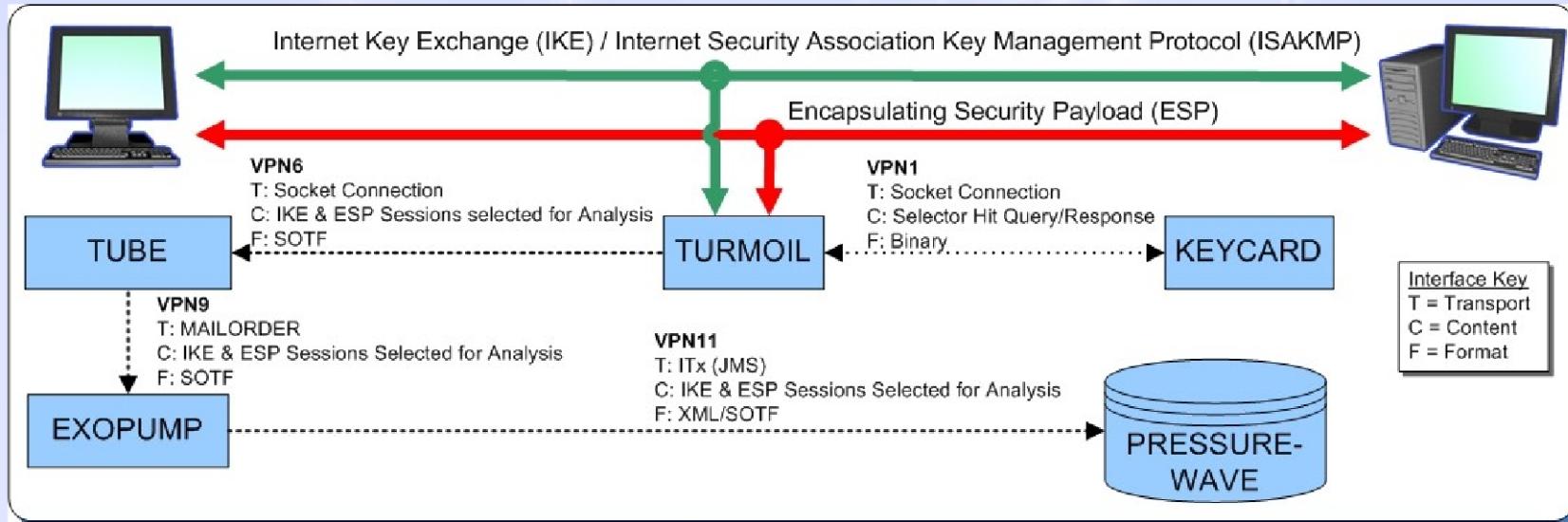


Dataflows and Interfaces - ESP Metadata





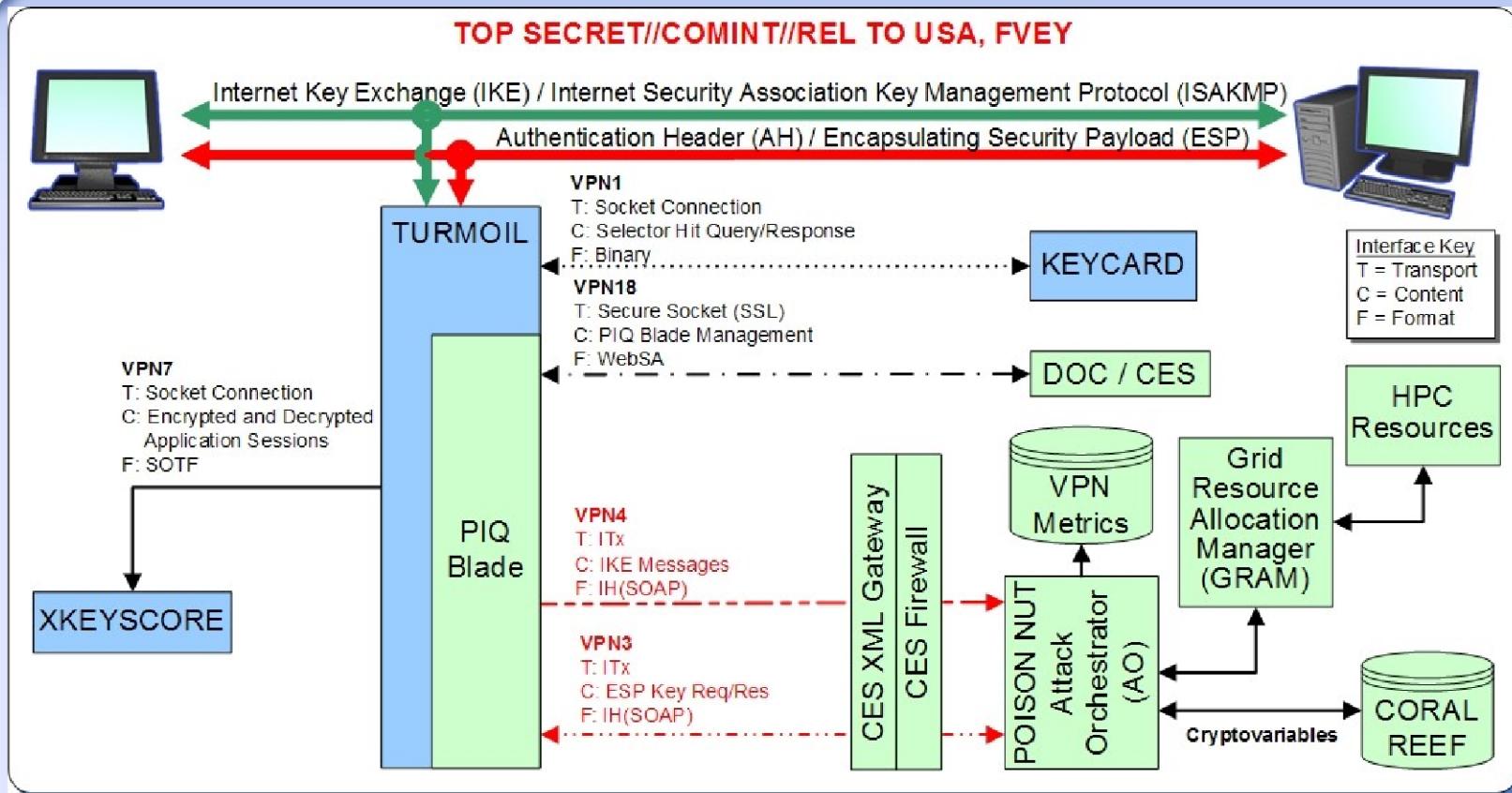
Dataflows and Interfaces - Analyze



- (U//FOUO) KEYCARD IP Target Action must be ANALYZE
- (U//FOUO) Full-take of IKE/ESP Sessions.
- (U//FOUO) No Analytic at this time

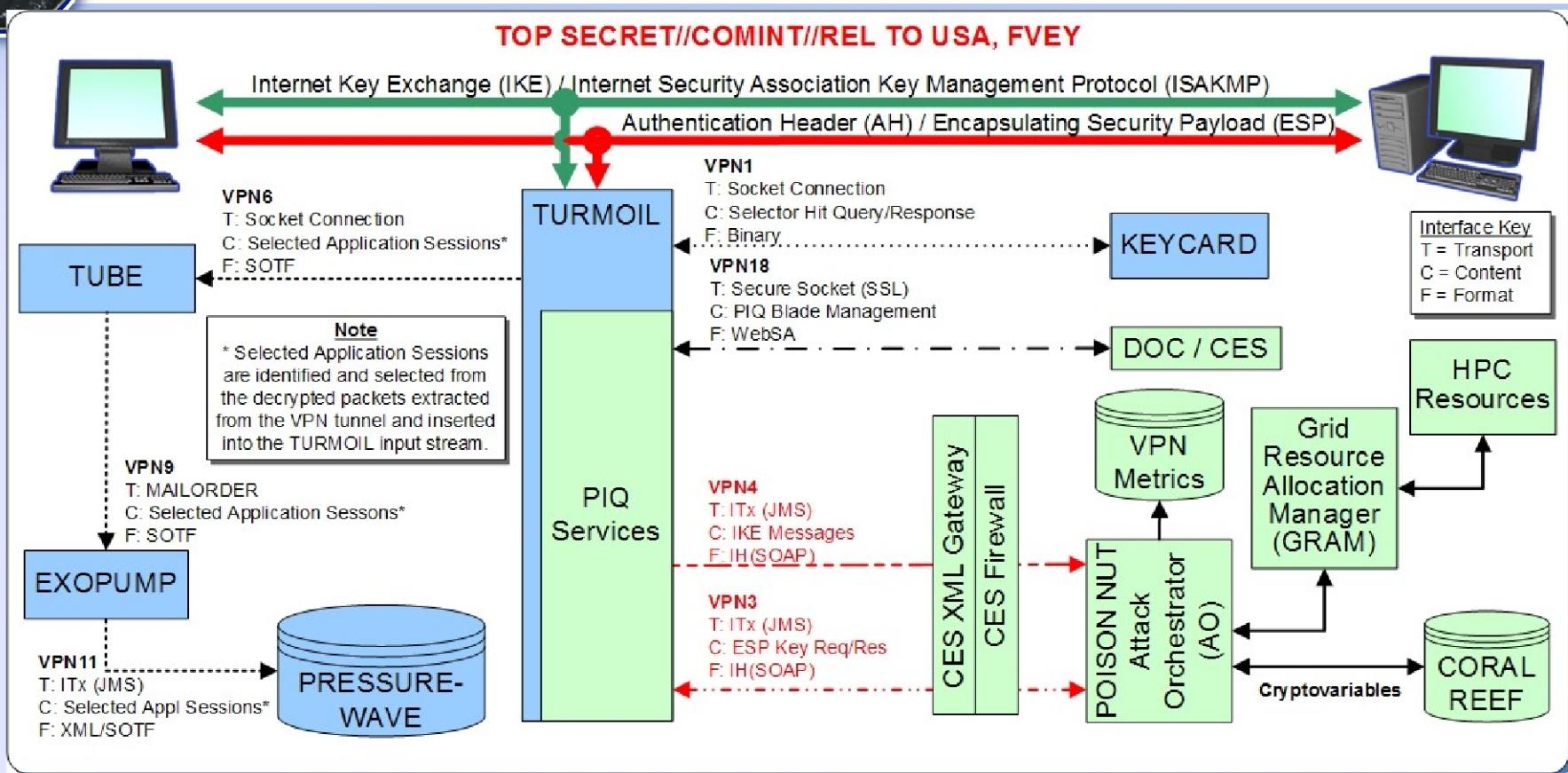


Dataflows and Interfaces - Survey



- (U//FOUO) KEYCARD IP Target Action must be TRANSFORM & SURVEY
- (TS//SI//REL) Candidate Sessions for Decryption include BME:
vpnID = "08000000-0000-0000-000000000001"
- (TS//SI//REL) Decrypted Sessions include BME:
vpnID ≠ "08000000-0000-0000-000000000001"

Dataflows and Interfaces - Transform

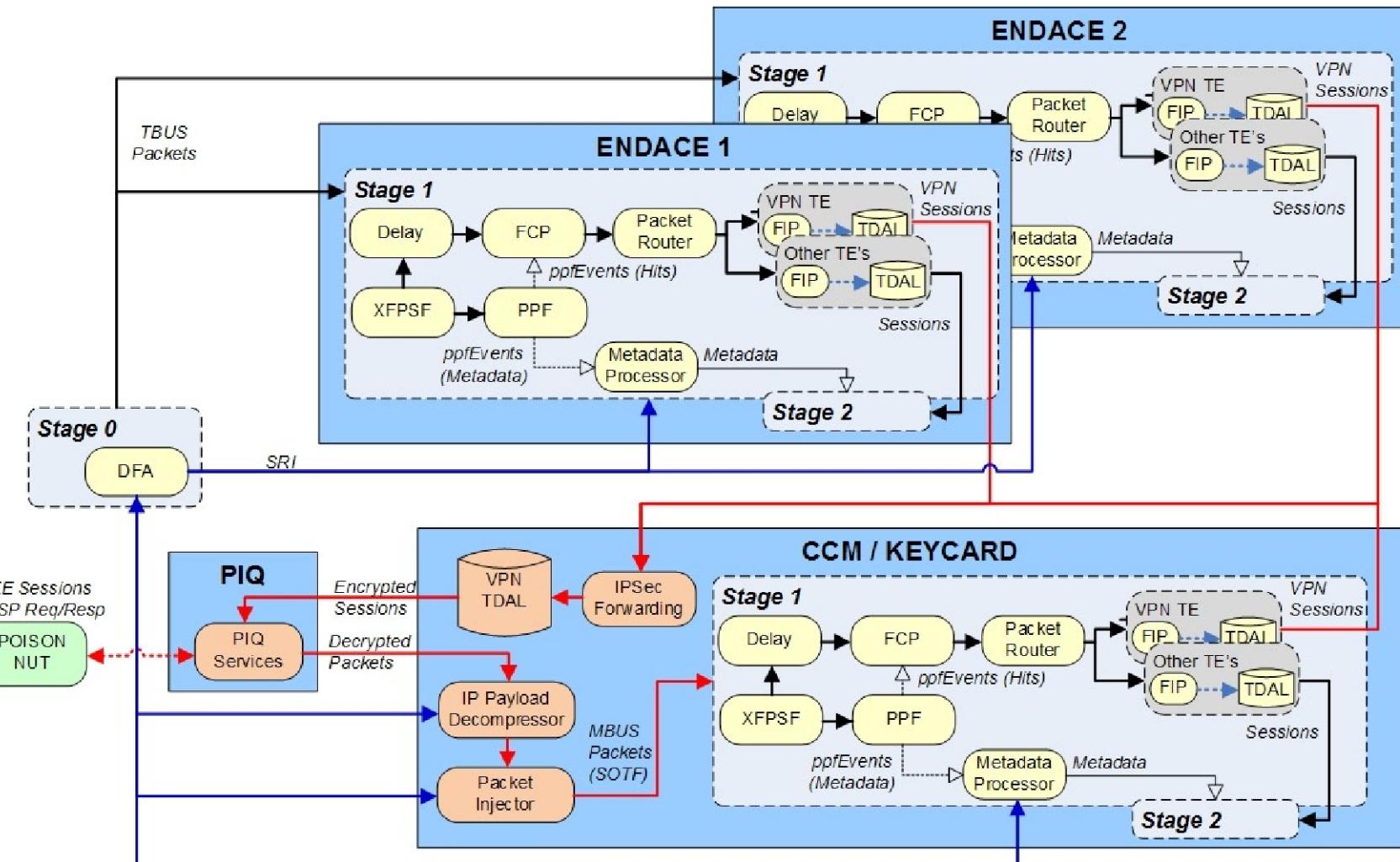


- (TS//SI//REL) PIQ Blade provides PIQ-Services, PICARESQUE ECI Compartmented
- (TS//SI//REL) Transform is Sanitization of Decrypt
- (S//SI//REL) VPN AH/ESP Session Transform capability is not available in Spin 12
- (U//FOUO) KEYCARD IP Target Action must be **TRANSFORM**
- (TS//SI//REL) Decrypted sessions have BME vpnID ≠ “08000000-0000-0000-0000-000000000001”



VPN on Dell LPT

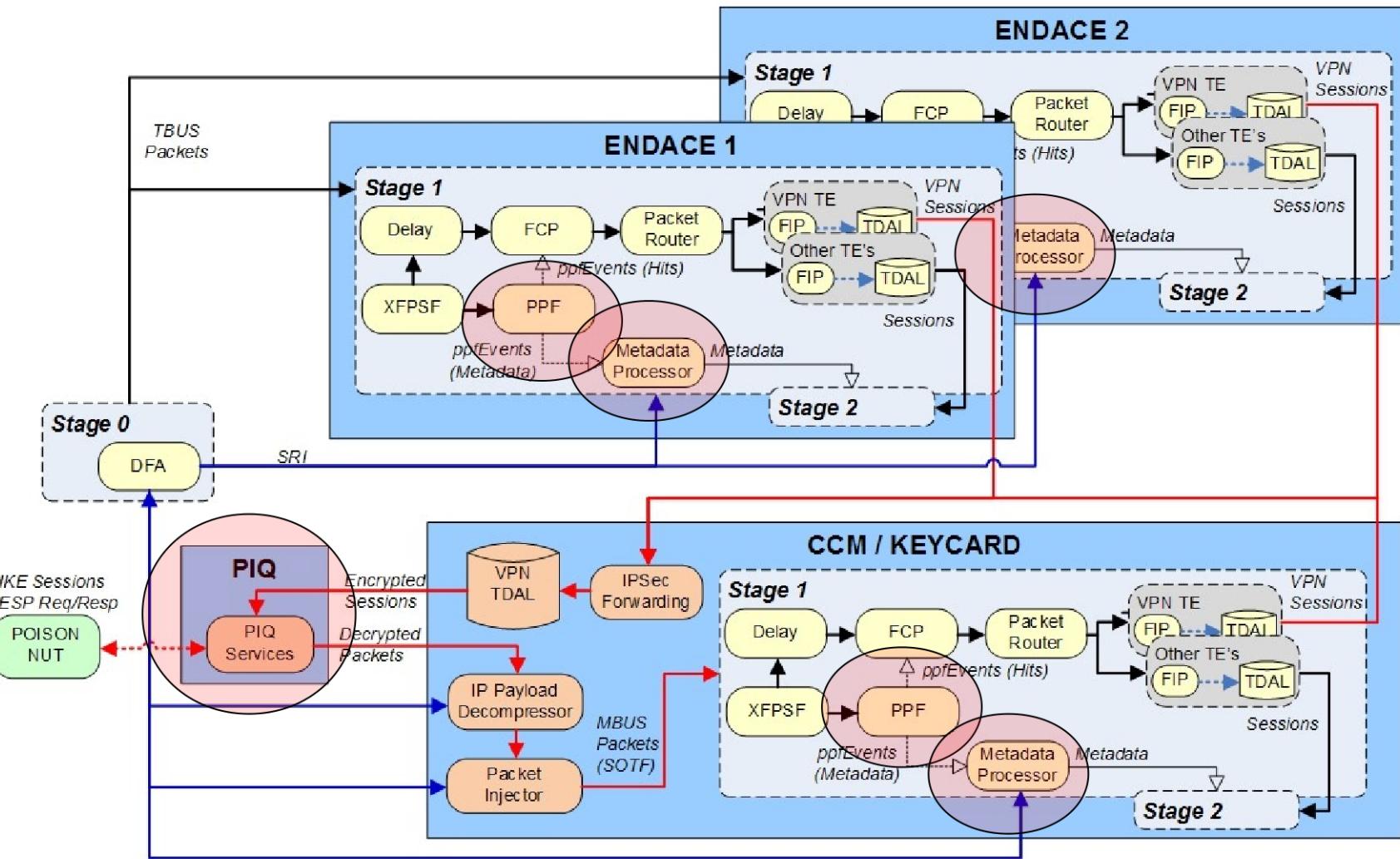
TOP SECRET//COMINT//REL TO USA, FVEY





VPN on Dell LPT

TOP SECRET//COMINT//REL TO USA, FVEY





Sample stats : 14-22 Oct 2009

System	KeyRequests	KeyResponses	KeyNotRecovered	Packets Decrypted
MHS_DEV	8076	0	0	0
MHS_LIVE	26501	12200	0	8041883
MHS_LPT	1725	0	0	0
SMK6	43087	4755	0	1413532



IKE Metadata Sequence

TOP SECRET//COMINT//REL TO FVEY

